IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

JOHN BONELL, individually and on behalf of similarly situated individuals,	)	
Plaintiff,	)	No. 19-cv-02339
v.	)	Honorable John Robert Blakey
COFFEE MEETS BAGEL, INC., a Delaware corporation,	)	**Jury Demanded**
Defendant.	)	

FIRST AMENDED CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff John Bonell brings this First Amended Class Action Complaint and Jury Demand against Coffee Meets Bagel, Inc., ("Defendant" or "CMB") on his own behalf, and on behalf of a class and subclass of individuals, to seek redress for CMB's conduct leading up to, surrounding, and following a data vulnerability and breach incident that exposed the personal information of millions of its customers. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

INTRODUCTION

1. Coffee Meets Bagel, Inc. owns and operates an online dating application called "Coffee Meets Bagel" (the "App").

2. CMB's App is used by millions of individuals throughout the United States. Prior to using CMB's App, users must provide their full names, email addresses, gender, registration date, and other sensitive information (collectively, "PII") to CMB.

3. Starting in late 2017 and ending in the middle of 2018, CMB suffered a series of

data beach incidents (the “Data Vulnerability” period), resulting in the unauthorized disclosure of the PII of over six million (6,000,000) of CMB’s customers.

4. CMB’s Data Vulnerability allowed unauthorized criminal third-parties to gain access to CMB information technology systems and extract the PII of millions of customers.

5. Following the Data Vulnerability, the PII of millions of CMB’s customers was listed for sale on the “dark web,” *i.e.* the black market of the internet.

6. Even though the Data Vulnerability was present by at least early 2017, CMB failed to reasonably detect and notify affected customers until February 2019.

7. CMB’s lax cybersecurity procedures allowed hackers to obtain access to Plaintiff’s and other customers’ PII. This PII should have been secured by adequate levels of protection and should not have been susceptible to unauthorized access via the Data Vulnerability.

8. As a result of CMB’s conduct in failing to reasonably prevent, detect, thwart, or mitigate the subject Data Vulnerability, Plaintiff and the other class members have suffered both pecuniary and non-pecuniary injury.

PARTIES

9. Defendant Coffee Meets Bagel, Inc., is a Delaware corporation that is transacting and conducting, and intentionally seeks to transact and conduct, business throughout Illinois, including in this District.

10. At all relevant times, Plaintiff John Bonell has been a resident and citizen of the State of Illinois.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this matter pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) *et seq.*, because this case is a class action in which the

matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are greater than 100 putative class members; at least one putative class member is a citizen of a state other than Defendant; and none of the exceptions under subsection 1332(d) apply.

12. This Court may assert personal jurisdiction over Defendant because it conducts and intentionally seeks to conduct business within this district, because it intentionally sought, stored, and undertook to protect the PII of a substantial number of Illinois residents, and because its conduct as alleged herein resulted in actual harm to a substantial number of Illinois residents.

13. Venue is proper in this District because Plaintiff resides in this District and a substantial part of the events giving rise to Plaintiff's claims occurred in this District.

FACTS SPECIFIC TO PLAINTIFF

14. Seeking to participate on the CMB App, Plaintiff created an account with Defendant. As a precondition to using CMB's App, Plaintiff was required to provide his PII to CMB.

15. Although Plaintiff was able to successfully and adequately participate on the CMB App and access the content and services contained on the CMB App, CMB failed to safeguard the PII Plaintiff initially provided to it.

16. On February 14, 2019, CMB sent an email to Plaintiff informing him that his PII was compromised during the subject Data Vulnerability. According to CMB's own email, it did not detect the Data Vulnerability until February 11, 2019, even though the Data Vulnerability existed in at least early 2017.

17. Thus, CMB failed to detect the Data Vulnerability for no less than a year from when the Data Vulnerability first materialized.

18. Plaintiff's PII, like that of millions of other class members, was not only

compromised during the Data Vulnerability, but also listed for sale on the dark web.

19. CMB's failure to implement reasonable cybersecurity protocols that included adequate technical, administrative, and physical controls created the subject Data Vulnerability which allowed third-party criminals to directly access Plaintiff's and other customers' PII. For example, an adequate intrusion detection and prevention system would have alerted Defendant to the presence of the of the Data Vulnerability within a reasonable time, and adequate technical measures, such as encryption, would have sufficiently de-identified the subject PII. However, CMB failed to implement such measures.

20. Notably, Defendant not only failed to prevent the Data Vulnerability, but also failed to detect it for over a year, thereby greatly aggravating Plaintiff's and other customers' injuries and risk of identity theft.

21. Given the current prevalence of cybersecurity awareness, especially in light of constant, high profile data breaches, CMB knew of the risks inherent in capturing, storing, and using the PII of their customers and the consequences of the exposure of such PII to unauthorized third parties.

22. Security lapses, like the subject Data Vulnerability, harm consumers beyond increasing the likelihood of identity and financial theft—they are harmed by the fact that their personal information, such as emails, addresses, and phone numbers are connected with their names.

23. As security experts now know, the release of data breach victims' personal information, even personal information which on its own may not constitute "traditional" PII, to the black market not only increases the likelihood of identity theft, but also makes them an easy target for spammers and phishing campaigns. Thus, Plaintiff and the Class members will be subject

to imminent and ongoing, targeted spam and phishing attacks since the third-party criminals are not only armed with certain of their PII, but also armed with the knowledge that such PII is associated with active users and valid, recently accessed accounts.

24. Indeed, active and valid email addresses, particularly when associated with additional user information such as first and last name, are more valuable to cyber-criminals and more easily sold to nefarious actors than "unverified" PII.

25. Had CMB informed Plaintiff of the Data Vulnerability within a reasonable period of time following its inception, Plaintiff and the other members of the putative class would have been able to take actions to protect their PII from further misuse by identity thieves or spammers.

26. Plaintiff believed that CMB would take reasonable measures to secure his PII. Had Plaintiff known that CMB would fail to take reasonable safeguards to protect and secure his PII, he would not have agreed provide his PII to CMB.

27. CMB's failure to comply with reasonable data security standards provided CMB a benefit in the form of saving on the costs of compliance, but at the detriment of CMB's own customers, including Plaintiff, whose PII has been exposed in the Data Vulnerability, or otherwise placed at serious and ongoing risk of imminent misuse, fraudulent charges, constant spam attacks, and identity theft.

28. Since recently becoming aware of the Data Vulnerability, Plaintiff has taken time and effort to mitigate his risk of identity theft, including changing his account passwords and monitoring his credit and other financial information to guard against fraudulent attempts to open credit cards or other financial accounts in his name.

29. Plaintiff has also been harmed by having his PII compromised and faces the imminent and impending threat of future additional harm from the increased threat of identity theft

and fraud due to his PII being sold, misappropriated, or otherwise misused by unknown parties, including ongoing targeted spam and phishing attacks.

30. Plaintiff has also experienced other pecuniary and non-pecuniary injury as a result of CMB's conduct leading up, surrounding, and following the breach, including mental anguish as when thinking about what would happen if his identity is stolen as a result of the Data Vulnerability.

CLASS ACTION ALLEGATIONS

31. Plaintiff brings this action on behalf of himself and a Class and Subclass (together, "Class" unless otherwise noted) defined as follows:

> **The Class:** All individuals whose PII was in the possession of Defendant, or any of their subsidiaries and/or agents, during the Data Vulnerability.
>
> **The Illinois Subclass:** All individuals in Illinois whose PII was in the possession of Defendant, or any of their subsidiaries and/or agents, during the Data Vulnerability.

32. **Numerosity**: Upon information and belief there are thousands, if not more, members of the Class. Defendant claims on its website to have made over 978,000 introductions in 2017 in Chicago alone.[1]

33. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the putative Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether CMB adequately safeguarded Plaintiff's and the Class members' PII;

b. Whether Plaintiff and the Class members were notified of the Data Vulnerability within a reasonable period and through a reasonable method;

c. Whether there was an unauthorized disclosure of the Class members' PII;

[1] *See* Coffee Meets Bagel, *CMB Year Review: Farewell 2017, Hello 2018!*, COFFEE MEETS BAGEL BLOG, https://s3.amazonaws.com/static.cmb.com/images/Chicago_banner.jpg.

d. Whether Defendant's cybersecurity prevention, detection, and notification protocols were reasonable under industry standards;

e. Whether Defendant's PII storage and protection protocols and procedures were reasonable under industry standards;

f. When Defendant became aware of the unauthorized access to Plaintiff's and the Class members' PII; and

g. Whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*.

34. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class and has retained counsel competent and experienced in complex class action. Plaintiff has no interest antagonistic to those of the other Class members, and Defendant has no defenses unique to Plaintiff.

35. **Appropriateness**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. The damages suffered by the individual Class members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual Class members to obtain effective relief from Defendant's misconduct. Even if the Class members could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action maximizes efficiencies and minimizes burdens and expenses on the parties and the judicial system.

COUNT I
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*. (on behalf of Plaintiff and the Illinois Subclass)

36. Plaintiff realleges the foregoing allegations as if fully set forth herein.

37. Pursuant to Section 530/20 of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*. ("ICFA"), CMB was required to implement and maintain reasonable security measures to protect the Plaintiff's and the Illinois Subclass members' PII.

38. Despite representing to Plaintiff and the Illinois Subclass members that it would not only implement commercially reasonable measures to protect their PII but also notify them if any security issues were to arise, CMB nonetheless failed to fulfill such representations, including by failing to timely detect the Data Vulnerability.

39. CMB's conduct was unfair because CMB represented its cybersecurity practices in a manner which induced Plaintiff and the Illinois Subclass members to provide their PII. Plaintiff and the Illinois Subclass members were thus under the impression that their PII was secure, that the CMB App would be regularly and reasonably vetted for anomalies, such as the subject Data Vulnerability, and that in the event of an anomaly, CMB would diligently discover and notify them of the same.

40. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant's unlawful conduct and violations of the ICFA and analogous state statutes.

41. Wherefore, Plaintiff prays for the relief set forth below.

COUNT II
Breach of Contract Implied-In-Fact (on behalf of Plaintiff and the Class)

42. Plaintiff realleges the foregoing allegations as if fully set forth herein.

43. Plaintiff and the Class members and CMB, by operation of their respective conduct and actions, entered into a contract implied-in-fact whereby Plaintiff and the Class members utilizing CMB App provided their PII as a precondition thereto, and CMB, representing its cybersecurity practices, was obligated to reasonably secure, monitor, and otherwise handle such PII.

44. As part of these agreements implied-in-fact, CMB agreed to safeguard and prevent the unauthorized disclosure of Plaintiff's and the Class members' PII.

45. CMB's failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures, including the failure to even detect the Data Vulnerability for over a year, constitutes a breach of such agreements.

46. Plaintiff and the Class members would not have provided and entrusted their PII to CMB in the absence of an agreement with CMB to reasonably safeguard their PII and to reasonably detect security issues, such as the subject Data Vulnerability.

47. Plaintiff and the members of the Class fully performed their obligations in provisioning the requested PII to CMB.

48. CMB breached the contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII and failing to reasonably and timely detect the Data Vulnerability.

49. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breaches of contract.

50. Wherefore, Plaintiff prays for the relief set forth below.

COUNT III
Breach of Implied Contract
(on behalf of Plaintiff and the Class) (in the alternative to Count II)

51. Plaintiff realleges the foregoing allegations as if fully set forth herein.

52. Plaintiff and the Class members were required to provide their PII to CMB prior to using the CMB App. To the extent that it is found that CMB did not have an express contract implied-in-fact with Plaintiff and the Class members, CMB entered into implied contracts with Plaintiff and the Class members whereby, by virtue of such requirement to provide their PII, CMB was obligated to take reasonable steps to secure and safeguard such PII, and obligated to take reasonable steps following an unauthorized disclosure to detect the same.

53. CMB's failure to implement adequate and reasonable data privacy and cybersecurity protocols constitutes a breach of an implied contract between CMB and the Class members.

54. Plaintiff and the Class members would not have provided and entrusted their PII to CMB in the absence of an agreement with CMB to reasonably safeguard their PII and to reasonably detect security issues, such as the subject Data Vulnerability.

55. Plaintiff and the members of the Class fully performed their obligations under their implied contracts with CMB.

56. CMB breached the implied contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII and failing to reasonably and timely detect the Data Vulnerability.

57. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of CMB's breaches of contract.

58. Wherefore, Plaintiff prays for the relief set forth below

COUNT IV
Negligence
(on behalf of Plaintiff and the Class)

59. Plaintiff realleges the foregoing allegations as if fully set forth herein.

60. CMB required Plaintiff and Class members to provide their PII.

61. At all relevant times, CMB had a duty, or undertook/assumed a duty, to implement a reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to safeguard the PII of the Plaintiff and the Class members, and to prevent the unauthorized access to and disclosures of the same.

62. Also, upon accepting and storing Plaintiff's and Class members' PII, CMB undertook and owed a duty to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so. This duty included, among other things, designing, implementing, maintaining, and testing CMB's cybersecurity systems to ensure that Plaintiff's and the Class members' PII was reasonably secured and protected.

63. CMB breached the aforementioned duties in, including but not limited to, one or more of the following ways:

a. Failing to implement reasonable data privacy and cybersecurity measures to secure its or Plaintiff's and Class members' email accounts, including failing to require adequate multifactor authentication and encryption;

b. Failing to implement a reasonable data privacy and cybersecurity protocol, including adequate procedures for preventing cybersecurity threats and/or detecting such threats in a timely manner;

c. Failing to reasonably comply with applicable state and federal law concerning its data privacy and cybersecurity protocol; and

d. Otherwise failing to act reasonably under the circumstances and being negligent with regards to its conduct in preventing, detecting, and disclosing the subject Data Vulnerability.

64. CMB knew, or should have known, that its data privacy and cybersecurity protocol failed to reasonably protect Plaintiff and the Class members' PII and failed to reasonably detect anomalies concerning the same.

65. As a direct result of CMB's aforesaid negligent acts and omissions, Plaintiff and the Class members suffered injury and damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, the loss of the benefit of their bargain with CMB, and pecuniary injury in the form of expense to mitigate the disclosure and significantly increased risk of exposure of PII to nefarious third parties.

66. Wherefore, Plaintiff prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class and Subclass set forth above, respectfully request the Court order relief and enter judgement against Defendant:

A. Certifying the Class and Subclass identified above and appointing Plaintiff as Class representative and the undersigned counsel as Class counsel;

B. Awarding Plaintiff and the Class and Subclass appropriate relief, including actual, statutory, compensatory, and/or punitive damages;

C. Requiring Defendant to furnish identity fraud monitoring and mitigation services for a reasonable period of time;

D. Granting injunctive relief requiring Defendant to implement commercially reasonable cybersecurity measures to properly guard against future cyberattacks and to provide prompt, reasonable notification in the event of such an attack;

E. Requiring Defendant to pay Plaintiff's and the Class's and Subclass's reasonable attorneys' fees, expenses, and costs; and

Any such further relief as this Court deems reasonable and just.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: June 11, 2019

Respectfully Submitted,

JOHN BONELL, individually and on behalf of a
Class and Subclass of similarly situated individuals

By: /s/ Jad Sheikali
One of Plaintiff's Attorneys

Eugene Y. Turin
David L. Gerbie
Jad Sheikali
MCGUIRE LAW, P.C. (#56618)
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
eturin@mcgpc.com
dgerbie@mcgpc.com
jheikali@gmail.com

Attorneys for Plaintiff and the Putative Class and Subclass